Volume 8
Issue 1
CREIGHTON INTERNATIONAL AND COMPARATIVE LAW JOURNAL

Cyber Civilians as Combatants

By: Christopher E. Bailey[1]

I. CYBER WARFARE: AN EMERGING AREA OF STATE PRACTICE

The United States, like many other countries, has used increased numbers of government civilians to accompany and support deployed military forces over the past decades.[2] In fact, there is evidence that sensitive cyber operations require personnel with advanced skills working against a target set over a long period of time,[3] suggesting that civilians may be better suited for certain roles over military personnel subject to rotational service personnel policies. This raises the issue

[1] Mr. Christopher E. Bailey is a faculty member at the National Intelligence University specializing in national security law, processes, intelligence ethics, and strategy. He is a 2008 graduate of NIU's Denial & Deception Advanced Studies Program and the U.S. Army War College. He is licensed to practice law in California and the District of Columbia, and is a member of the National Security Law section, American Bar Association. He has LLM degree in National Security & U.S. Foreign Relations Law from the George Washington University School of Law. All statements of fact, analysis, or opinion are the author's and do not reflect the official policy or position of the National Intelligence University, the Department of Defense or any of its components, or the U.S. government.

[2] COLONEL RONDA G. UREY, CIVILIAN CONTRACTORS ON THE BATTLEFIELD, 1 (Carlisle Barracks, PA: U.S. Army War College, 2005). *See also* William Welsh, *Cyber Warriors: The Next Generation*, DEFENSE SYSTEMS, Jan. 23, 2014, http://defensesystems.com/articles/2014/01/23/next-generation-cyber-warriors.aspx (discussing the expanding use of civilian and military personnel in both the offensive and defensive aspects of cyber warfare).

[3] Shane Harris, *How the NSA Became a Killing Machine*, THE DAILY BEAST, Nov. 9, 2014, http://www.thedailybeast.com/articles/2014/11/09/how-the-nsa-sorta-won-the-last-iraq-war.html (discussing the partnership between the U.S. military and the National Security Agency to support offensive cyber operations in Iraq and how those operations were instrumental in removing over 4,000 insurgents from the battlefield). *See also* Dune Lawrence, *The U.S. Government Wants 6,ooo New 'Cyberwarriors' by 2016*, BLOOMBERG BUSINESS, Apr. 15, 2014, http://www.bloomberg.com/bw/articles/2014-04-15/uncle-sam-wants-cyber-warriors-but-can-he-compete (discussing the long lead times for education and training, as well as the high pay commanded by private sector employment); U.S. Dep't. of Defense, *DoD Cyber Strategy*, 18, (Apr. 2015) ("DoD must recruit and retain highly-skilled civilian personnel, including technical personnel for its total cyber workforce").

whether the use of civilians, as agents of a belligerent nation-state, to conduct cyber operations in international armed conflict violates international humanitarian law (IHL).[4] If a civilian serving as an intelligence officer at the National Security Agency (NSA), the U.S. Cyber Command (CYBERCOM), or a deployed location conducts an otherwise lawful cyber operation, is that person, if later captured, entitled to prisoner of war (POW) status and combatant immunity?[5] This article argues that government civilians can serve in such combatant roles without violating international law. Indeed, this article argues that civilians serving as cyber-combatants may be better positioned than military personnel to meet the requirements of military necessity,[6] while respecting the rights of non-combatants and regulating the conduct of the parties to the conflict.[7]

---

[4] In the U.S. view, the established principles of IHL apply in cyberspace, even though there may be disagreement on its application in certain situations. Harold Hongju Koh, Legal Adviser to the U.S. Department of State, at the U.S. CYBERCOM Inter-Agency Legal Conference, Ft. Meade, MD (Sept. 18, 2012) available at http://www.state.gov/s/l/releases/remarks/197924.htm. *See also* U.S. Dep't. of Defense, Office of the General Counsel, 997 Law of War Manual (June 2015) (recognizing that IHL provides only a general guide in emerging, technologically advanced areas of State practice such as cyber warfare). *See generally*, TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt, ed., New York: Cambridge University Press, 2013) (the *Tallinn Manual*, a multi-year collaborative effort by a group of international experts sponsored by the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, offers a persuasive restatement of IHL in a cyber-context; the manual provides extensive commentary on each "rule," with majority and minority opinions on each point).

[5] The use of loosely connected civilians in cyber militias or a volunteer corps would raise separate and distinct legal issues under the 1949 Geneva Conventions, and is outside the scope of this article. *See*, for example, *Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949* (Geneva Convention III), Art. 4(A)(2), Aug. 12, 1949, 75 U.N.T.S. 135 (which requires that such groups be commanded by a person responsible for his subordinates, to have a fixed distinctive sign, to carry arms openly, and to conduct their operations in accordance with the laws and customs of war).

[6] According to the International Committee of the Red Cross, "the destruction or seizure of the property of an adversary is prohibited, unless required by imperative military necessity." Int'l Comm. of the Red Cross, *Customary International Humanitarian Law, Volume I: Rules*, Rule 50 (Cambridge, 2005).

[7] The general principles underpinning IHL (*jus in bello*) are necessity, distinction and proportionality. The principle of necessity requires that:

> Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

This article focuses on the use of civilians as cyber-combatants in armed conflict between belligerent nation-states, as defined by the 1949 Geneva Conventions.[8] Indeed, it is important to identify the timing and types of operations that might be conducted by civilian cyber practitioners. First, international armed conflict could involve stand-alone cyber operations, as well as cyber operations that precede and support conventional attacks.[9] In one example, civilian cyber-combatants may be permitted to conduct certain collection activities during peacetime or a period of tensions which might not be permissible for them to later conduct "during" an armed conflict.

The 1977 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflict (Additional Protocol I), Art. 52(2), June 8, 1977, 17512 U.N.T.S. 3. The principle obligating attackers to distinguish between combatants/military objectives and civilians/civilian objects is embodied in the Additional Protocol I, Article 48. The proportionality principle requires parties to refrain from launching any attack that may be expected to cause incidental injury or collateral damage that "would be excessive in relation to the concrete and direct military advantage anticipated …." *Id*., Article 57 (2)(iii). While the United States is not a signatory to Additional Protocol I, the principles regarding the protection of civilians likely reflect customary international law. *See generally* Nils Melzer, Int'l. Comm. Of the Red Cross, *Interpretive Guidance on The Notion of Direct Participation in Hostilities Under International Humanitarian Law*, (Feb. 2009); Michael Matheson, Deputy Legal Adviser, U.S. Dep't. of State, Remarks at Sixth Annual American Red Cross-Washington College of the Law Workshop (Jan. 22, 1987).

[8] Under the Geneva Conventions of 1949, Common Article 2, an international armed conflict is defined as a "declared war or any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of August 12, 1949* (Geneva Convention I) Aug. 12, 1949, 75 U.N.T.S. 31; *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of August 12, 1949* (Geneva Convention II) Aug. 12, 1949, 75 U.N.T.S. 85; *Geneva Convention Relative to the Treatment of Prisoners of War of August 12, 1949* (Geneva Convention III) Aug. 12, 1949, 75 U.N.T.S. 135; *and Geneva Convention Relative to the Protection of Civilian Persons in Time of War of August 12, 1949* (Geneva Convention IV) Aug. 12, 1949, 75 U.N.T.S. 287.

[9] In the 2008 conflict over South Ossetia, Russia reportedly conducted small-scale computer network attacks against Georgia over a two-month period preceding conventional military operations. In such a situation, a victim-state would have difficulty characterizing such preliminary attacks as a "use of force" under Article 2 (4) of the Charter of the United Nations, as well as attributing the attacks to state sponsorship. Heather Harrison Dinniss, *Cyber Warfare and the Laws of War*, 54-5 (Cambridge, UK: Cambridge University Press, 2012).

[10] In addition, some cyber operations—especially ones with a limited effect during a period of tensions before a conflict—might be considered as falling short of the use of force threshold warranting the application of IHL.[11] Second, many intelligence activities that might be conducted during the armed conflict (e.g., cyber collection and exploitation) might also be non-destructive in character and would not necessarily raise the same level of concerns as either attacks or defensive actions that result in the spread of terror, injury to people, or damage to property.[12] In other words, what is the permissible range of cyber activities for a civilian cyber practitioner during an international armed conflict?

---

[10] Simon Chesterman, *The Spy Who Came in from the Cold War: Intelligence and International Law*, 27 MICH. J. INT'L L. 1071 (2006) (arguing that certain peacetime intelligence activities—like collection (espionage)—do not violate international law, but its constitutive acts may violate foreign domestic laws). *See also* Jeffrey H. Smith, Keynote Address, *State Intelligence Gathering and International Law*, 28 MICH. J. INTL. L. 543 (2007). However, members of the armed forces, in time of armed conflict, who fall "into the power of an adverse Party while engaging in espionage shall not have the right to the status of prisoner of war and may be treated as a spy." Additional Protocol I, *supra* note 7, Art. 46 (1). In a like manner, a person who enters a foreign nation while in civilian disguise for the purpose of carrying out acts of sabotage could be treated as either a criminal or an unlawful combatant. *See* Ex Parte Quirin, 317 U.S. 1 (1942) (eight Nazi saboteurs had landed by submarine and had changed into civilian clothes before capture; all were treated as unlawful combatants). Clearly, a civilian intelligence officer conducting a range of offensive cyber operations—entirely from friendly territory—cannot be considered as a spy or a saboteur, at least in the classic sense of the term, but there are questions about how to characterize that person's activity during an international armed conflict.

[11] U.N. Charter art. 2(4). Article 51 further recognizes the inherent right of self-defense, if an "armed attack" occurs. This raises a question about the transition point from *jus ad bellum* (conflict management) to *jus in bello* (the application of IHL); at what point does a cyber attack become serious enough that a breach of peace has occurred that warrants an armed response? *See also* Michael N. Schmitt, *Computer Network Attack and the Use of Use in International Law: Thoughts on a Normative Framework*, 37 COLUM. J. OF TRANSNAT'L L. 885 (1998-99) (analyzing the nature of cyber computer network operations under international law and positing the need for an alternative normative framework based upon an assessment of the consequences caused by such operations).

[12] Additional Protocol I, *supra* note 7, Art. 51, provides that the "civilian population and individual civilians shall enjoy general protection against dangers arising from military operations." Article 51 (2) provides that the "civilian population as such, as well as individual civilians shall not be the object of attack." Article 51 (5) proscribes indiscriminate attacks "which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

Cyber operations may involve either offensive (attack) or defensive actions. The term "cyber attack" is used here to refer to "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[13] Cyber attacks may range from a Distributed Denial of Service (DDoS) attack[14] with temporary effects, such as the recent service outage in North Korea,[15] to a broader, more destructive attack as in the 2010 Stuxnet attack against the Iranian nuclear facilities.[16] Cyber defensive actions may be entirely passive or involve some level of response (e.g., a counter attack or a proportionate countermeasure[17]) against attacking enemy systems. In

[13] NAT'L RESEARCH COUNCIL, TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBER ATTACK CAPABILITIES 20 (William A. Owens, Kenneth W. Dam & Herbert S. Lin, 2009. Additional Protocol I, *supra* note 7, Art. 49 (1), defines "attacks" as "means of violence against the adversary, whether in offense or in its defense." Under the *Tallinn Manual,* Rule 30, a "cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects." Schmitt, *Tallinn Manual, supra* note 4. This opens up a broad range of computer network operations against civilian objects—all with temporary effects—that may be conducted by civilian cyber practitioners during an international armed conflict without necessarily violating the prohibition against direct participation in hostilities. Dinniss, *Cyber Warfare, supra* note 9, at 196-202.

[14] A DDoS attack is a "technique that employs two or more computers, such as bots of a botnet, to achieve a denial of service from a single or multiple targets." Schmitt, *Tallinn Manual, supra* note 4, at 259.

[15] Cecilia Kang, *North Korean Web Goes Dark Days After Obama Pledges Response to Sony Hack*, THE WASHINGTON POST (Dec. 22, 2014), http://www. washingtonpost.com/ business/economy/north-korean-web-goes-dark-days-after-obama-pledges-response-to-sony-hack/ 2014/12/22/b76fa0a0-8a1d-11e4-9e8d-0c687bc18da4_story.html.

[16] Michael B. Kelley, *The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought*, BUSINESS INSIDER (Nov. 20, 2013), http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11. *See also* PAUL K. KERR ET AL., CONG. RESEARCH SERV., R41524, THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY (2010). The Stuxnet attack, unlike the temporary effects in the earlier 2007 cyber attack on Estonia or the 2008 cyber attack on Georgia, raises the *jus ad bellum* issue whether the attack was a "use of force" in violation of Article 2(4) of the Charter of the United Nations and whether Iran had the right to respond to an "armed attack" under Article 51.

[17] "A State injured by "an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State." Schmitt, *Tallinn Manual, supra* note 4, Rule 9. The commentary to Rule 9 then notes that two separate tests of proportionality have been advanced, one that the countermeasure must be proportionate to

any case, from the victim's perspective, it is often difficult to distinguish a cyber collection activity that maps out a friendly system for later attack, from a cyber exploitation that delivers a payload to that system (e.g., malware or a logic bomb) designed to activate at a later date, and from an attack that is actually intended to impair that system on either a temporary or permanent basis.[18]

Cyber operations are an emerging and revolutionary area of State practice; the belligerents in a future armed conflict are unlikely to forsake its advantages. Cyber operations offer technologically advanced belligerents a means to bring about favorable outcomes short of costly, labor and resource intensive, conventional military operations.[19] Moreover, during an armed conflict, cyber operations offer a valuable complement to broader on-going conventional operations, especially in making such operations more efficient and effective. Even so, with the complex, inter-connected and dual-use[20] nature of the Internet in a technologically advanced country, it means that cyber attackers will have to spend increased time and resources in the planning and conduct of operations. Indeed, cyber practitioners must consider not only the direct

---

the breach and the second that the countermeasure must be commensurate to the injury suffered. *Id. at* Comment 7.

[18] According to the National Research Council, cyber attack and cyber exploitation require a "vulnerability, access to that vulnerability, and a payload to be executed–-the only difference is in the payload to be executed." Owens, *supra* note 13. According to one report, computer network exploitation involves data extrapolation or manipulation, while computer network attack is the military parlance for offensive operations; the report indicates that the concepts are closely related and sometimes indistinguishable. CATHERINE A. THEOHARY & ANNE I. HARRINGTON, CONG. RESEARCH SERV., R 43848, CYBER OPERATIONS IN DOD POLICY AND PLANS: ISSUES FOR CONGRESS 16 (2015).

[19] Some nation-states may prefer the strategic ambiguity offered by cyber offensive operations, combined with plausible deniability, as a means of projecting coercive force against adversaries with greater conventional military power. Indeed, attackers have a range of tactics that can combine the structure and vulnerabilities of the Internet with secretive techniques, such as tunneling, data log destruction and false flag activities, that greatly complicate attribution to the responsible parties. Scott J. Shackelford & Richard B. Andres, *State Responsibility For Cyber Attacks: Competing Standards for a Growing Problem,* 42 GEO. J. INT'L L. 4 (Summer 2011).

[20] This term is not defined in international law. Dinniss notes that once an object meets the definition of a military objective it becomes liable to attack despite its concurrent military and civilian usage. Dinniss, *Cyber Warfare, supra* note 9, at 193. However, the civilian aspects of a dual-use system (e.g., an integrated power grid that supports a hospital and a military installation) are considered in the proportionality analysis. This problem is also complicated by the fact that military forces often use communications systems that under private sector control, making it difficult for an attacker to know whether a system is used by the military and to what extent.

effects of a proposed attack, but also the so-called "knock-on"—the second and third order—effects of an attack.[21] A cyber practitioner must, therefore, conduct a sophisticated reconnaissance and analysis of a proposed target to ensure that the target is properly identified, and that injury to civilians and damage to civilian objects is minimized over a broad period.[22] This leads to issues regarding the permissible range of cyber operations that may be conducted by civilian cyber practitioners. In other words, when does a civilian practitioner become a cyber-combatant and what kinds of things can that person do without violating international law?

II. INTERNATIONAL HUMANITARIAN LAW

A. INTRODUCTION

International law does not prohibit civilians from participating in cyber operations during an international armed conflict.[23] Nonetheless, the nature and extent of a person's participation does have legal consequences in terms of his targetability, POW status, and right to immunity from prosecution for otherwise lawful acts of war (i.e., combatant immunity) by the capturing belligerent. However, the principles and rules of IHL have developed from centuries of State practice and international agreement, and have been largely focused on conventional, kinetic operations by uniformed military forces. Cyber operations raise new and revolutionary issues, not necessarily answered by existing law. Indeed, some aspects of inter-state cyber operations may call for a reexamination of State practice and may suggest a need for new understandings in customary international law.

B. COMBATANT STATUS: PRISONERS OF WAR & COMBATANT IMMUNITY

[21] *Id. at* 207-9.
[22] *Id. at* 206-7.
[23] Schmitt, *Tallinn Manual, supra* note 4, Rule 95.

The 1949 Geneva Conventions (Geneva III) creates two legal classifications for individuals within the context of an international armed conflict; people can be classified as either combatants or civilians.[24] Article 4, as applicable to international armed conflict, defines legal combatants as:

> A. Prisoners of war, in the sense of the present Convention, are persons belonging to one of the following categories, who have fallen into the power of the enemy:
>
> (1) Members of the armed forces of a Party to the conflict, as well as members of militias or volunteer corps forming part of such armed forces.
> (2-3) …
> (4) Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization, from the armed forces which they accompany, who shall provide them for that purpose with an identity card similar to the annexed model.
> (5-6) ….[25]

Here, civilian cyber practitioners, even if located in the United States at places like the NSA headquarters at Fort Meade, Maryland, could be considered as persons "who accompany the armed forces." In fact, it is public knowledge that the NSA is a combat support agency of the Department of Defense (DoD)[26] that conducts a range of important national intelligence missions, to include support of deployed forces through reach back operations.[27] In that sense, the headquarters with its entire military/DoD civilian workforce is a valid military objective for an opposing state-actor and its destruction would severely impair U.S. military operations during an international armed conflict. In any case, civilian employees working at that location could be targeted by an adversary based upon the principles of necessity, distinction, and proportionality.

[24] Geneva Convention III, *supra* note 8.
[25] *Id. at* Art. 4.
[26] 10 U.S.C. § 193 (Combat Support Agencies: Oversight).
[27] U.S. DEP'T. OF DEFENSE, *JOINT AND NATIONAL INTELLIGENCE SUPPORT TO MILITARY OPERATIONS* (JOINT PUBLICATION 2-01), at B-21 to B-25 (Oct. 7, 2004).

The 1977 Additional Protocol I, to which the United States is not a signatory, provides additional guidance on combatant status and, in many areas, likely reflects customary international law.[28] Article 43 (1) provides that:

> The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct or its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which, *inter alia*, shall enforce compliance with the rules of international law applicable in armed conflict. [29]

Article 43 (3) then allows for a slightly more expansive definition of the term "combatant"; it can permit the inclusion of civilians into the "armed forces": "Whenever a Party to a conflict incorporates a paramilitary or armed law enforcement agency into its armed forces it shall so notify the other Parties to the conflict."[30] While civilian employees of the Department of Defense may not be members of a uniformed military service, the employees are part of the "groups and units which are under a command responsible" for their conduct. The civilian cyber practitioners of the Department, especially at "paramilitary" combat support agencies such as the NSA and U.S. CYBERCOM and which have senior level military leadership, can be "incorporated" into the armed forces.[31] The senior level military leadership can ensure that cyber operations meet mission

---

[28] Abraham D. Sofaer, Legal Adviser, U.S. Department of State, *Agora: Protocol I to the Geneva Conventions*, 82 AM. J. INT'L L. 784, (Oct. 1988).

[29] Additional Protocol I, *supra* note 7, Art. 43. Articles 43-45 likely also reflect customary international law regarding the combatant distinction between "Members of the armed forces" and "persons who accompany the armed forces …." Matheson, *supra* note 7.

[30] Additional Protocol I, *supra* note 7, Art. 43 (3).

[31] There is a split of opinion on whether this provision applies to intelligence or other government agencies not having a law enforcement function. The majority of the International Group of Experts that drafted the *Tallinn Manual* did not believe that a party could incorporate such agencies, while a minority of experts disagreed. Schmitt, *Tallinn Manual, supra* note 4, Rule 26, at Comment 15. In a like manner, there is a split of opinion regarding the prohibition against the use of mercenaries, a term that could be applied to a limited class of civilian cyber practitioners who conduct offensive cyber operations. Matheson, *supra* note 7. Under Additional Protocol I, *supra* note 7, Art. 47, a mercenary is defined as a person recruited to fight in an armed conflict who takes part in hostilities, but "(d) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; [and] (e) is not a member of the armed forces of a

requirements consistent with IHL, using the best qualified personnel—military or civilian—to accomplish that mission.

This extension of existing law is supported by a 2013 reported decision of the German Federal Prosecutor General when considering criminal charges in which a drone strike—allegedly conducted by the Central Intelligence Agency (CIA)—killed a German national (B.E.) in Afghanistan.[32] Initially, the Prosecutor General found that B.E. had been killed in a non-international armed conflict and that he had been killed consistent with the principles of necessity, distinction and proportionality. The Prosecutor General then held that the CIA officers, even if the drone lacked military markings, qualified as members of the armed forces under Additional Protocol I, Article 43.[33] The Prosecutor General noted that the CIA officers were not integrated into the military command structure, but did act under "responsible command" and were a "unit comparable to, and closely connected with the regular military in terms of their objectives, armament, and organization."[34] The Prosecutor General explained that this functional definition of the term "armed forces" was also consistent with the notion that the officers performed a "continuous combat function"[35] and were integrated into the armed forces on a *de facto* basis.

This informed opinion by the Prosecutor General could be applied with greater force and effect to the use of DoD civilian cyber practitioners at the NSA, the U.S. CYBERCOM, and at deployed locations with the U.S. military. The NSA and the Command are currently co-located at Fort Meade, with the NSA providing the Command with support for "target and access

---

Party to the conflict …." Thus, the prohibition against using mercenaries would not rule out the use of U.S. citizens as civilian cyber-combatants, but it would bar the employment of foreign nationals in that capacity.

[32] Bundesgerichtshof [BGH] [Federal Court of Justice] July 23, 2013, 157, International Law Reports [ILR] 722 (Ger.).

[33] The court noted that the conflict was non-international in character, raising the applicability of Additional Protocol II. Nonetheless, the court found that Additional Protocol I, Article 43, was applicable to non-international armed conflicts. *Id. at* 758.

[34] *Id.*

[35] The ICRC uses the "continuous combat function" test to assess a person's participation in a non-international armed conflict. According to the ICRC, "Continuous combat function requires lasting integration into an organized armed group acting as the armed forces of a non-State party to an armed conflict. Thus, individuals whose continuous function involves the preparation, execution, or command of acts or operations amounting to direct participation in hostilities are assuming a continuous combat function." Melzer, *supra* note 7, at 34.

development, enabling DoD cyberspace operations and execution."[36] This statement implies that the NSA currently provides a broad range of combat support activities, while the Command conducts the actual operations. According to press, there is "lasting integration" between the two organizations, "with personnel moving freely between the two" operations centers.[37] Indeed, the dual-hatted role of the NSA Director and Commander, U.S. CYBERCOM, ensures that the work of the two organizations is closely coordinated and that personnel—both DoD civilian and military—work together to perform operational missions.[38] In effect, government civilians and contractors are likely already performing support functions just short of the combat functions of the CIA officer operating a drone. At deployed locations, the relationship between the civilian and military personnel is likely stronger, with civilians integrated into military organizations from supervisory-level to work unit and subject to discipline by senior military officers, with all personnel sharply focused on the mission. This means that, consistent with the object and purpose of Article 43, civilian cyber practitioners can provide a broader range of "combat functions" whether at reach back or deployed locations.

Article 44 (3) provides additional guidance on the distinction problem in cyber warfare; it initially obligates combatants "to distinguish themselves from the civilian population while they are engaged in an attack or in a military operation preparatory to an attack."[39] Article 44 (3)(a) then recognizes that there situations in where, "owing to the nature of the hostilities an armed combatant cannot so distinguish himself," but requires that he carry his arms openly "during each engagement" and "during such time as he is visible to the adversary while engaged in a military deployment preceding launching of an attack in which he is to participate."[40] However, a cyber-

[36] U.S. DEP'T. OF DEFENSE, *DOD CYBERSPACE POLICY REPORT*, REPORT TO CONGRESS PURSUANT TO THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011, SECTION 934 (Nov. 2011).
[37] Ellen Nakashima, *NSA, Cyber Command Leadership Should be split up, officials advocate*, THE WASHINGTON POST, Nov. 29, 2013, https://www.washingtonpost.com/world/national-security/nsa-us-cyber-command-leadership-should-be-split-up-officials-advocate-according-to-sources/2013/11/29/09fb5c02-5904-11e3-8304-caf30787c0a9_story.html.
[38] U.S. CYBERCOM, BEYOND THE BUILD DELIVERING OUTCOMES THROUGH CYBERSPACE: THE COMMANDER'S VISION AND GUIDANCE FOR U.S. CYBER COMMAND, (U.S. Dep't. of Defense, June 2015).
[39] Additional Protocol I, *supra* note 7, Art. 44 (3).
[40] *Id.* at Art. 44 (3)(a). This exception originated with the concern for guerrilla groups and insurgents in enemy-occupied territory. Watts, *supra* note 24, at 7. Unlike the "lawless" bands

combatant employs "arms" that are by necessity concealed within near instantaneous electronic transmissions and "he" is rarely "visible" to the adversary "during each engagement." Thus, Article 44 (3)(a) recognizes that there are some situations in which an "armed" combatant cannot distinguish himself, although it retains two archaic State practices that are not relevant for cyber warfare.

Clearly, neither the 1949 Geneva Conventions nor the 1977 Additional Protocol I were written with consideration for the requirements of cyber warfare. In practice, offensive cyber operations are conducted with great speed and by necessity on an anonymous basis, with the adversary often not even realizing that he is under cyber attack, much less with any understanding that the person sitting at a keyboard half a world away might or might not be "distinguishing" himself through the wearing of a uniform or by carrying arms openly. A person's status as a legal or an illegal combatant should not turn on considerations not visible to the adversary; in other words, the principle of distinction that originated with the wear/non-wear of a uniform and other symbols visible to an adversary on the battlefield who would be obligated to make his own good faith targeting decisions, is outmoded in the "remote, over-the-horizon engagements" endemic in cyber war.[41] Professor Sean Watts argues that "[f]ar more than the outward appearance of individuals conducting [computer network attacks], distinction in CNA demands attention to the actual conduct of the attack—the target chosen, pathways of entry, the means used to achieve destruction or harmful effects."[42]

Instead, scholars and practitioners should consider a functional ("continuous combat function") test to assess whether certain civilians are part of the "armed forces" by the nature and purpose of their activities. Cyber-combatants serving under responsible command and conducting State sponsored and directed cyber operations consistent with IHL should be considered legal combatants without regard to military or civilian status.[43] In part, this functional test would further

---

that sometimes operate on the battlefield, government civilians, whether working in the United States or at deployed locations, are subject to U.S. criminal law, as well as agency disciplinary regulations.

[41] Watts, *supra* note 24, at 15.

[42] *Id*.

[43] Press reporting indicates that the Director of the NSA, traditionally a serving general/flag officer in the U.S. military, will remain "dual-hatted" as the Commander, U.S. CYBERCOM for the foreseeable future. Sean Gallagher, *White House: NSA and Cyber Command to stay under*

the interests of IHL by ensuring that the best qualified personnel are conducting sensitive, technical operations and are doing so consistent the principles of necessity, distinction and proportionality. In part, this functional test would also eliminate a "uniformed" recognition test that has no practical meaning to an adversary who defends against cyber attacks mounted by practitioners who are not, in any case, physically present and "distinguishable" in a traditional sense.

C. COMBATANT STATUS: DIRECT PARTICIPATION IN HOSTILITIES

Civilian cyber practitioners often perform a broad range of functions in support of military operations, raising an important question about the threshold between combatant and non-combatant activities. The parties to an armed conflict are obligated to observe the general principle of distinction; that is, in an effort to respect and protect the civilian population and civilian objects, the parties must at all times direct operations only against military objectives.[44] The 1977 Additional Protocol provides that civilians shall not be the object of an attack "unless and for such time as they take a direct part in hostilities."[45] This means that a civilian cyber practitioner who is not participating in hostilities is entitled to a protected status, like any other civilian. This also means that a civilian who does participate in hostilities can become a lawful target, at least for such time as he directly participates in hostilities.[46]

---

one boss, ARS TECHNICA, December 13, 2013, http://arstechnica.com/tech-policy/2013/12/white-house-nsa-and-cyber-command-to-stay-under-one-boss/.

[44] ICRC, *Customary International Humanitarian Law*, *supra* note 6, Rule 1 requires that the "parties to the conflict must at all times distinguish between civilians and combatants. Attacks may only be directed against combatants. Attacks must not be directed against civilians." *See also* Additional Protocol I, *supra* note 7, Art. 48 ("the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives").

[45] Additional Protocol I, *supra* note 7, Art. 51 (3). This point likely reflects customary international law. Matheson, *supra* note 7.

[46] Schmitt, *Tallinn Manual, supra* note 4, Rule 35. Rule 35 provides: "Civilians enjoy protection against attack unless and for such time as they directly participate in hostilities." *See also* Herbert Lin, "Cyber Conflict and International Humanitarian Law," 94 INT'L REV. OF THE RED CROSS 886, 525-26 (Summer 2012) (raising a spectrum of civilian involvement in cyber hostilities).

The concept of direct participation in hostilities (DPH) has raised nettlesome questions that have bedeviled practitioners, academics, and jurists.[47] In many cases, it may be difficult to assess whether certain preparatory steps, to include cyber reconnaissance of an enemy system or the preparation of the malware, constitutes "participation" in or has a direct causal relationship to hostile acts. In other cases, it may be difficult to decide whether a cyber practitioner has employed a "weapon," especially if that attack uses an inherently dual-use "object" like software code to produce non-destructive effects.[48] Some scholars have even suggested that DPH involves not only "the delivery of violence," but also actions aimed at protecting personnel, material and facilities.[49] Thus, one must ask what cyber activities can be construed as DPH?

The International Committee of the Red Cross (ICRC) defines the "constitutive elements" of DPH as:

> 1. The act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or

[47] An analogous debate has focused on persons supporting the employment of improvised explosive devices (IEDs) by insurgents who are often not clad in military uniforms, albeit in non-international armed conflict. Here, a person's activities might range from a less direct connection to an attack, such as the financing of bomb-makers and the actual making of bombs, to more direct connections in delivering the bomb to the attack location and manning the observation point while waiting for the target to appear. This situation, sometimes referred to the farmer-by-day, fighter-by-night, or a revolving door, problem centers on persons who hide among the civilian population, claiming its protective status, while waiting for an opportune time to attack. This also raises questions about the "duration" of a person's DPH. Clearly, there is often a subtle transition, open to competing interpretations, regarding the transition from civilian to combatant status. *See*, for example, GEOFFREY S. CORN ET AL., THE WAR ON TERROR AND THE LAWS OF WAR 44-54 (New York: Oxford University Press, 2009).

[48] Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SEC. L. & POL'Y 115 (2014) (concluding that an effort to treat all cyber techniques as weapons is impractical and that practitioners should instead focus on how the cyber capability will be used in a particular context). While international law bans certain weapons, such as poison gases and biological weapons, Additional Protocol I obligates States to conduct an Article 36 assessment of all new weapons, means and methods of warfare. Thus, the question arises whether certain lines of software code, to include even minor changes to an existing code, constitute a new "weapon" and require a legal review. *See also* INT'L. COMMITTEE OF THE RED CROSS GENEVA, A GUIDE TO THE LEGAL REVIEW OF NEW WEAPONS, MEANS AND METHODS OF WARFARE: MEASURES TO IMPLEMENT ARTICLE 36 OF THE ADDITIONAL PROTOCOL I OF 1977, (Jan. 2006).

[49] Dinniss, *Cyber Warfare*, *supra* note 9, at 163.

> destruction on persons or objects protected against direct attack (threshold of harm), and
> 2. there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part (direct causation), and
> 3. the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (belligerent nexus).[50]

This three-part conjunctive test, focused on the threshold of harm, direct causation, and the belligerent nexus, provides a useful starting point for assessing whether and to what extent a civilian cyber practitioner is conducting combatant activities.[51]

The key issue involves the nature of the cyber activities that civilian practitioners may engage in during an international armed conflict without violating the prohibition against DPH. In practice, a broad range of non-destructive cyber activities, to include intelligence collection, exploitation, and passive defense activities, especially ones not reaching the threshold of harm or having a direct causal relationship to such harm, probably would not violate the prohibition. On the other hand, cyber attacks, as well as counter-attacks and proportionate (defensive) countermeasures, could well constitute hostile acts that would have an adverse, direct effect on an adversary's on-going military operations or overall military capacity. Here, even temporary effects and non-destructive activities, such as part of a DDoS attack, could provide friendly forces with a momentary advantage that could be exploited with well-timed conventional operations. Heather Dinniss, a research fellow at the Swedish National Defense College, also notes that less direct civilian assistance in the design and execution of cyber attacks could constitute DPH where it could be linked to a particular attack.[52]

In practice, hostile acts committed by a civilian cyber practitioner would result in that person losing his protected status as a civilian—making him a combatant—and permit the

[50] Melzer, *supra* note 7, at 16.
[51] This three-part test has also been adopted by the International Group of Experts for application to cyber warfare. Schmitt, *Tallinn Manual*, *supra* note 4, Rule 35.
[52] Dinniss, *Cyber Warfare*, *supra* note 9, at 167.

adversary to target him, his facilities and activities under the principle of necessity. This analysis highlights the point that certain activities can transform a civilian cyber practitioner into a cyber-combatant; this analysis does not, however, answer the question of whether that cyber practitioner is a legal or an illegal combatant. And, the fact that a civilian may have participated in hostilities through cyber attacks does not necessarily mean that his acts are punishable as war crimes.

D. THE RULE AGAINST PERFIDY

The rule against perfidy, that is acts inviting an adversary's detrimental reliance on a protected status, has been a traditional concern under international law; the rule also raises important distinction issues for cyber practitioners.[53] Does it violate the rule for a "civilian" to conduct a cyber attack? Or, for that matter, can military personnel portray themselves as enemy "civilians" to cause an adversary to do something that he would not otherwise do? Does it violate the rule for a practitioner—military or civilian—to conduct an attack through the use of a "civilian" object? The key issue here is the extent to which the rule is an anachronism no longer applicable to modern cyber warfare.

The rule has its roots in the 1907 Hague Regulations, Article 23 (b), which provides that it is forbidden "to kill or wound treacherously individuals belonging to the hostile nation or army …."[54] The 1977 Additional Protocol I, Article 37, expanded on the basic rule, proscribing a range of activities to include the feigning of surrender, incapacitation, civilian status, or a protected status involving the "signs, emblems or uniforms" of U.N. personnel or neutral parties with the intent (i.e., a *mens rea*) to betray that confidence.[55] Article 39 then proscribes the use of neutral flags, emblems, insignia or uniforms, or that of the enemy while engaging in attacks. Ruses, on the other hand, are defined as acts intended to mislead (deceive) an enemy, but do not misuse a protected status or symbol; ruses are not prohibited.[56] Hence, one could argue that cyber practitioners are

[53] Sean Watts, *Law-of-War Perfidy*, 219 MIL. L. REV. 106 (2014).
[54] Convention (IV) Respecting the Laws and Customs of War on Land and its Annex: Regulation Concerning the Laws and Customs of War on Land, Oct. 18, 1907, IHL-19-EN.
[55] Additional Protocol I, *supra* note 7, Art. 37.
[56] *Id*. at Art. 39 (2).

misusing a protected status, that belonging to civilians and/or civilian objects, when conducting cyber attacks and are therefore subject to prosecution for perfidy.

In a sense, all cyber operations involve some level of secrecy and deception, largely in an effort to gain a decision advantage over an adversary. A digital attacker does not distinguish himself as a "combatant," enabling an attacker to disguise his identity and make it difficult for a defender to know if a transmission is actually a treacherous attempt to kill him. One tactic could involve hacking into a militant cell phone network to send false text messages from one militant to one of his colleagues (e.g., making allegations that a third colleague is not actually pious or has committed some other sinful act, especially against the group). The use of this tactic can sow confusion, distrust or hatred within a network, even bringing about its collapse.[57] A second tactic might involve web spoofing, the posting of false messages on an adversary's website. By hacking into a group's website, the cyber attacker could send false messages to a terrorist leader, directing him to a meeting site with a "colleague" but where he might actually be "meeting" with (i.e., be captured or killed by) a uniformed special operations team.[58] This example could, however, constitute an act of perfidy if the special operations team had actually planned to ambush and kill the terrorist leader, especially if the kill team had been clad entirely in civilian mufti. Thus, it might be more accurate to say, from the victim's perspective, that a cyber attacker has neither military nor civilian status; the identity of the person behind a cyber persona is an unknown and that a recipient who trusts unencrypted communications or suspicious transmissions does so at his own peril.

The use of a civilian object to conceal a cyber weapon (e.g., the data contained on a thumb drive) could be considered a lawful ruse in at least two different ways. First, the cyber attack could be permissible if it were treated like the permissible use of civilian clothing by a combatant to mask his approach to an enemy soldier, but still showing some kind of combatant "insignia" (e.g., something analogous to an "armband" worn by French partisans in World War II) in the period

[57] ERIC SCHMITT & THOM SHANKER, COUNTERSTRIKE: THE UNTOLD STORY OF AMERICA'S CAMPAIGN AGAINST AL QAEDA 147-48 (New York: St. Martin's Griffin, 2012).
[58] *Id*.

immediately preceding and during the attack.[59] Here, it might be an acceptable ruse to mark the bait as something that would have military applications, such as "engineering texts," "tools program," or a Windows update. Second, the cyber attack could be permissible if the "weapon" was not used to "kill or wound" individuals treacherously; in other words, if the attack had been designed to capture someone or if the attack was not the proximate cause of a person's death or wounding, it could be treated as a ruse. Like the identity of the cyber attacker, the status of the "object" is generally an unknown and cannot be trusted until verified. In any case, it would likely violate the rule against perfidy by using a thumb drive, disk or other device that is marked as "U.N. Inspections Guide,"[60] "Red Crescent,"[61] or as something clearly non-military such as an update to a popular iTunes app.

In a certain sense, the rule against perfidy seems like an anachronism, reminiscent of the pre-cyber battlefields, especially when one considers that the rule developed because of actions like the misuse of a white flag of surrender or the use of medical vehicles to mount a direct kinetic attack. Nevertheless, cyber warfare imposes new and challenging requirements for practitioners, often requiring changes in State practice with an evolving understanding of legal obligations. Thus, while existing law still allows a range of novel ruses, many of which can be analogized to acceptable past practices, other practices, such as a treacherous killing or the misuse of a protected symbol like that of the Red Crescent, will still be proscribed.

E. ASSESSMENT

Civilian cyber practitioners can serve in a range of combatant roles, while retaining combatant immunity, without violating the rule against perfidy. This proposed expansion of State practice is consistent with the continuous combat function test used by the ICRC and is supported

[59] W. Hays Parks, *Special Forces' Wear of Non-Standard Uniforms*, 4 CHICAGO J. OF INT'L LAW 493, 521-24 (2003), http://chicagounbound.uchicago.edu/cjil/vol4/iss2/16 (explaining that the wear of civilian clothing by special operations personnel can constitute an act of perfidy if done for the purpose and result of "killing treacherously").
[60] Additional Protocol I, *supra* note 7, Art. 37 (1)(d).
[61] The perfidious misuse of the distinctive emblem of the Red Cross, Red Crescent or Red Lion and Sun would be a war crime under Geneva Convention I, *supra* note 8, Art. 53; such misuse would also be a grave breach under the 1977 Additional Protocol I, *supra* note 7, Art. 85 (3)(f).

by the informed decision of the German Federal Prosecutor regarding combat operations conducted by CIA officers in Afghanistan/Pakistan. This functional test would also change the focus from a "uniformed" recognition test that has no practical meaning to an adversary who defends against cyber attacks conducted by practitioners who are not "distinguishable" in a traditional sense. Instead, practitioners should ensure that the best qualified personnel—military or civilian—are used in the design and delivery of offensive and defensive cyber operations to effectuate the underlying principles of necessity, distinction and proportionality during operations. This proposed practice could provide enhanced mission effectiveness, and also respect and protect the rights of non-combatants and non-belligerents.

III. TOWARD A MODERN CYBER WARRIOR

The modern cyber warrior, as an agent of a belligerent power in an international armed conflict, can be a serving military member or a civilian government employee consistent with and based upon a good faith extension of existing law. IHL, based on both customary international law and treaty, has evolved over the centuries, largely in response to changes in State practice and the contemporary sense of obligations (*opinio juris*) in modern warfare. Many important principles, such as necessity, distinction and proportionality, must now be adapted to the new and unique requirements of technologically advanced cyber warfare. The fundamental problem for cyber-combatants, military or civilian, is the principle of distinction. A "functional" (e.g., a continuous combat function) test should be used to determine whether certain civilians are part of the "armed forces." This would allow cyber civilians to serve in combatant roles while also furthering the object and purpose of the 1949 Geneva Conventions and the 1977 Additional Protocol I—respecting and protecting the rights of non-combatants and non-belligerents—in international armed conflicts. Finally, this expanded view of the civilian cyber practitioner should also help the U.S. CYBERCOM in its efforts to recruit and retain a highly skilled workforce.